

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-186753

(P2003-186753A)

(43) 公開日 平成15年7月4日 (2003.7.4)

(51) IntCl. ⁷	識別記号	F I	テームコード (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 D 5 B 0 1 7
1/00		1/00	3 5 0 B 5 B 0 5 4
1/24		9/06	6 6 0 L 5 B 0 7 6

審査請求 未請求 請求項の数12 O L (全 12 頁)

(21) 出願番号 特願2001-388639(P2001-388639)

(22) 出願日 平成13年12月21日 (2001.12.21)

(71) 出願人 000104652

キヤノン電子株式会社

埼玉県秩父市大字下影森1248番地

(72) 発明者 甘利 隆

埼玉県秩父市大字下影森1248番地 キヤノ
ン電子株式会社内

(74) 代理人 100075292

弁理士 加藤 卓

Fターム (参考) 5B017 AA03 BA08 BB03 BB05 CA11
CA14

5B054 AA01 AA06 BB08

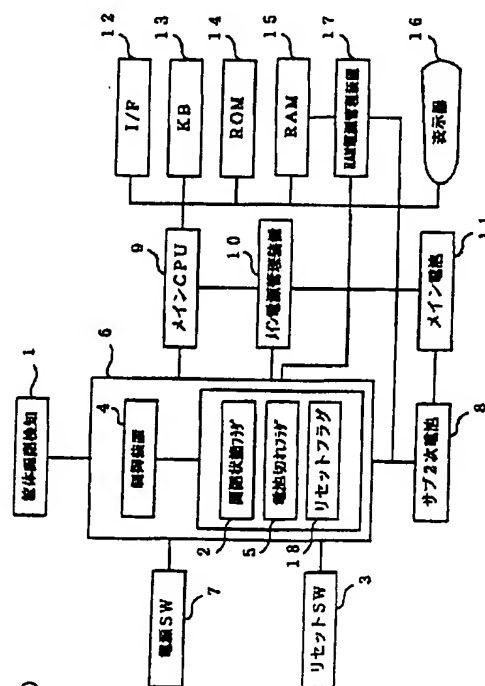
5B076 FC01 FD04

(54) 【発明の名称】 電子機器、電子機器の制御方法、および電子機器の制御プログラム

(57) 【要約】

【課題】 電子機器の耐タンパー性とメンテナンス性を両立できるようにする。

【解決手段】 筐体開閉状態フラグ2が過去の筐体の開放を示している時は、リセットスイッチ3によりリセット起動が指令された場合のみ所定のシェルを介した装置の操作を許容し、リセットスイッチ3によりリセット起動が指令されていない場合は装置の通常起動を禁止する。シェルを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、筐体開閉状態フラグ2を筐体の閉成を示す状態にリセットする。データ保護は、筐体開閉状態フラグ2が過去の筐体の開放を示している時は、記憶装置 (RAM 15) の内容を破壊するか、その複写を禁止することにより行なう。



(図1)

【特許請求の範囲】

【請求項 1】 筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器において、リセット起動を指令するリセット操作手段と、

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する制御手段を有することを特徴とする電子機器。

【請求項 2】 前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットすることを特徴とする請求項 1 に記載の電子機器。

【請求項 3】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊することを特徴とする請求項 1 に記載の電子機器。

【請求項 4】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止することを特徴とする請求項 1 に記載の電子機器。

【請求項 5】 筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器の制御方法において、

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止することを特徴とする電子機器の制御方法。

【請求項 6】 前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットすることを特徴とする請求項 5 に記載の電子機器の制御方法。

【請求項 7】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊することを特徴とする請求項 5 に記載の電子機器の制御方法。

【請求項 8】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止することを特徴とする請求項 5 に記載の電子機器の制御方法。

【請求項 9】 筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開

閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器の制御プログラムにおいて、

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する制御ステップを含むことを特徴とする電子機器の制御プログラム。

【請求項 10】 前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットする制御ステップを含むことを特徴とする請求項 9 に記載の電子機器の制御プログラム。

【請求項 11】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する制御ステップを含むことを特徴とする請求項 9 に記載の電子機器の制御プログラム。

【請求項 12】 前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する制御ステップを含むことを特徴とする請求項 9 に記載の電子機器の制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムに関するものである。

【0002】

【従来の技術】近年、電子商取引が普及するに伴い、電子機器のセキュリティが重要視されるようになってきた。

【0003】特に、PDA や携帯電話機、IC カードなどの携帯可能な電子機器に認証情報や個人情報を経絡し、これらの情報を用いて決済を行なう電子決済システムが考案されているが、このような電子決済システムの場合、電子機器自体を盗んで内蔵データを読み出すことにより、パスワード、個人情報、顧客情報や金銭情報などの機密性を要する内部データが流出してしまう危険性が考えられる。

【0004】このため、万が一電子機器が盗まれて第三者の手に渡っても操作できないように、電子機器の起動時にパスワードを要求したり、特別なキーオペレーションを設けたりすることで、内部の情報をプロテクトすることが考えられてきた。

【0005】しかし、パスワードや特別なキーオペレー

ションによるプロテクトは、機器自体が盗まれたような場合には、記憶装置を取り出して直接アクセスするような行為に対しては充分ではなく、また、機器が小型軽量であればある程、機器の紛失や盗難の可能性は高くなる。

【0006】また、不正に内部を改造またはリバースエンジニアリングすることにより、ソフトウェアやハードウェアに関する企業秘密やノウハウが流出する問題もある。

【0007】そこで、電子機器を盗んだ者が筐体を開けて、機密性を要する内部データを読み出したり、不正に内部を改造またはリバースエンジニアリングすることを防ぐために、耐タンパー（Tamper-Proof：いたずら防止あるいは不正防止）機能を備えた電子機器も考案されている。たとえば、一度でも機器の筐体が開放された場合、二度と動作しないように制御することにより、耐タンパー機能を実現することができる。

【0008】

【発明が解決しようとする課題】しかし、前述のように筐体が開放された場合二度と動作しないようにする従来の耐タンパー機能は、第三者の不正な改造やアクセスを防ぐという意味では効果があるが、不便である場合がある。たとえば、実際の運用時における正規のメンテナンス作業での筐体の開閉によっても同様に、以降の動作が出来なくなってしまうという不都合がある。

【0009】本発明の課題は、上記の問題を解決し、電子機器の耐タンパー性とメンテナンス性を両立できるようにすることにある。

【0010】

【課題を解決するための手段】上記の課題を解決するため、本発明によれば、筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムにおいて、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する構成を採用した。

【0011】あるいはさらに、前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の開成を示す状態にリセットする構成を採用した。

【0012】あるいはさらに、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する構成を採用した。

【0013】あるいはさらに、前記筐体開閉状態フラグ

が過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する構成を採用した。

【0014】

【発明の実施の形態】以下、図を参照して本発明の実施の形態を説明する。

【0015】【実施形態1】図1は、本発明を採用した携帯型電子機器の制御系の構成を、図2は、本発明を採用した携帯型電子機器の外観を示している。

【0016】本実施形態の携帯型電子機器の筐体は、図2に示すように上ケース21と下ケース20から構成されており、本携帯型電子機器を分解するためには、不図示の締結ネジを緩めて上ケース21と下ケース20を外す必要がある。後述の筐体開閉検知スイッチ1は、上ケース21と下ケース20の間の適当な位置に配置されており、上ケース21と下ケース20が閉じている状態ではClose信号を、上ケース21と下ケース20が空いている状態ではOpen信号を出力するように出来ている。図2中の符号を付した他の部材については、以下、図1に関する説明を参照されたい。

【0017】図1の制御回路において、筐体開閉検知スイッチ1は、上記の筐体が開けられたことを検出するスイッチであり、本携帯型電子機器の筐体を固定している締結ネジを緩めて、裏蓋を外した時にOpen信号を出力する。このOpen信号は、制御装置4へ割り込み信号として伝達される。

【0018】開閉状態フラグ2は、後述のサブCPU6に内蔵されているRAM15（後述のように、RAM15の内容は主電源遮断期間においてもバックアップ保持される）上に配置され、過去の筐体開閉検知スイッチ1の状態を記憶する。

【0019】リセットスイッチ3は、本発明の第1の実施形態である携帯型電子機器のハードウェアリセットを掛けるためのスイッチである。リセットスイッチ3を押すと、まず後述のサブCPU6に対してリセット信号が出力され、サブCPU6は割り込み処理により所定のリセットベクタから処理を開始する。

【0020】リセットフラグ18は、リセットスイッチ3が押され、サブCPU6がリセットスタートをした際にセットされるもので、サブCPU6は後述の電源スイッチ7からの信号によって後述のメインCPU9へ電源供給を開始する際に、このリセットフラグ18の状態を信号線を使ってメインCPU9へ伝える仕様になっている。なお、この情報はメインCPU9への電源供給を終了する際にクリアするようになっている。

【0021】制御装置4は、後述のサブCPU6の中心的存在であり、筐体の開閉状態や後述の電池切れフラグ5の値を元に、メインCPU9の電源管理を行なうための総合的判断を行なう機能を持つ。

【0022】電池切れフラグ5は、後述のサブCPU6に内蔵されたRAMの中に設けられている。具体的に

は、このフラグには特定パターンが書き込まれており、通常は後述のサブ2次電池8により内容がバックアップされているが、サブCPU6に電池切れが起きた時は保持されなくなるため内容が変わる。この変化を制御装置4で判断することにより、電池切れが発生したかを調べるフラグとして扱っている。

【0023】サブCPU6は開閉状態フラグ2、電池切れフラグ5、リセットフラグ18、制御装置4、不図示のROMやRAMやI/Fを内蔵している。開閉状態フラグ2、電池切れフラグ5、リセットフラグ18の状態は、信号線によってメインCPU9で取得することが可能であるが、それ以外のRAMおよびROMの内容はサブCPU6がパッケージ化されているため、外部から調べることは不可能である。なお、サブCPU6自体は、後述の電源スイッチ7の状態に関わらず、サブ2次電池8によって常に動作を続ける仕様となっている。

【0024】電源スイッチ7は、本携帯型電子機器の電源投入用スイッチであり、その指示信号はサブCPU6の制御装置4に入力され、サブCPU6内で電源供給の許可があった時に、後述のメイン電源管理装置10へ通電の指示が出る構成になっている。

【0025】サブ2次電池8は、サブCPU6の動作及び内蔵RAMのバックアップ、更にRAM15のバックアップに必要な電源を供給するためのものであり、後述のメイン電池11が外されても電源供給する機能がある。これにより、たとえば筐体を分解しようとしてメイン電池11を外しても、サブCPU6だけは動作を続けることが可能となり、筐体が開けられたかどうかを筐体開閉検知スイッチ1の過去の状態を記憶する開閉状態フラグ2により知ることができる。

【0026】メインCPU9は、後述のROM14の中のプログラムやデータ、及びRAM15の中の変数領域を使って、本携帯型電子機器の動作を制御する。

【0027】メイン電源管理装置10は、サブCPU6からの指示によりメイン電池11の電力をメインCPU9及び、インターフェース(I/F)12、キーボード13、ROM14、RAM15、表示器16などに供給する。

【0028】メイン電池11は、上記メイン電源管理装置10を経由してメインCPU9へ電源を供給する他に、メイン電池11が電子機器に装着されている間、サブ2次電池8へ充電を行なう。

【0029】インターフェース12は、本発明の携帯型電子機器が外部デバイス(携帯電話、メモ리카ード、プリンタなど)と接続する時に使用される。インターフェースの回路構成、通信方式は任意である。

【0030】キーボード13は、テンキーや入力キーなどから構成され、データ入力の際に用いられる。表示器16は、メインCPU9によって出力結果が描画されることによってメッセージや画像を表示する。

【0031】ROM14は、メインCPU9が処理を実行する際のプログラムやデータを格納し、RAM15は、メインCPU9が処理を実行する際、プログラム及び作業用の変数領域に用いられる。

【0032】RAM電源管理装置17は、サブ2次電池8からの電力をRAM15へ送るための機能があり、通常はRAM15へ通電し続けてバックアップする仕様になっている。サブCPU6からの指示によりこの電力供給はカットすることが出来、この場合、バックアップした内容を破壊することが出来る。

【0033】次に上記構成における動作について説明する。

【0034】図3は、本実施形態の携帯型電子機器の電源投入時のメインCPU9が実行するアルゴリズムを示している。

【0035】電源スイッチ7の押下によりサブCPU6に電源オンの指示が入ると、サブCPU6はメイン電源管理装置10へ電源供給の指示を出すことにより、メインCPU9が図3のステップS01から動作を開始する。

【0036】ステップS02では、サブCPU6内に設けられた電池切れフラグ5の内容を調べ、電池切れが起きている場合はステップS05へ分岐し、電池切れが起きていない場合はステップS03へ進む。

【0037】ステップS03では、サブCPU6内に設けられた筐体開閉状態フラグ2の内容を調べ、過去に筐体が開けられた形跡のある場合はステップS06へ、開けられたことのない場合はステップS04へ進む。

【0038】なお、本電子機器の電池がなくなった場合、サブCPU6内のRAMの内容は不定になるため、本筐体開閉状態フラグ2の正当性はなくなるが、このような場合は先のステップS02で無条件にデータ破壊の処理に進むので、内部データを不正に吸い上げることは不可能である。

【0039】ステップS04では、ステップS03で筐体が開けられたことがないと判断されて分岐して来た場合なので、本携帯型電子機器の正常通りの起動処理を行った後、不図示の本来の処理(アプリケーションプログラムの自動実行やシェルの起動)の処理へ制御を移す。

【0040】ステップS05では、セットされていた電池切れフラグ5をクリアする。これは、メインCPU9とサブCPU6を繋ぐ信号線を用いてメインCPU9からサブCPU6へ、電池切れフラグ2をクリアするコマンドを発行することにより行なう。

【0041】ステップS06は、本携帯型電子機器のRAM15の内容を破壊する処理である。これはたとえばメモリ内データを全て00でクリアする、または、RAM電源管理装置17からRAM15へ供給されるバックアップ電源を切ることにより行なう。

【0042】次に、ステップS07でリセットフラグ1

8を参照し、今回の起動がリセットスイッチ2を押下してから1回目の起動が否かを調べる。起動の直前にリセットスイッチ18が押下されていなかった場合、ステップS09でメインCPU9から信号線を使ってサブCPU6に電源オフ要求を出すことで、メイン電源管理装置10からの電源供給を切って装置全体の電源を遮断する。

【0043】ステップS07でリセット直後の起動であることが分かった場合、ステップS08でシェルを起動する。

【0044】図4は、ステップS08で起動されるシェルのアルゴリズムを示したフローチャートである。シェルとはオペレータがキーボード13から入力した文字列をコマンドとして解釈して、そのコマンドを実行するプログラムであり、たとえば、UNIX（商標名）においてはsh、cshなど、MS-DOSにおいてはCOMMAND.COMなどが代表的である。本実施形態においては、これら一般のシェルに機能を一部追加しており、以下のようなアルゴリズムになっている。

【0045】まず、ステップS12で、本携帯型電子機器のキーボード13からコマンド文字列が入力される。

【0046】次にステップS13で、この文字列が記憶装置のフォーマット（初期化）を命令するコマンド名に一致する場合はステップS14へ分岐、それ以外の時はステップS15へ分岐する。記憶装置のフォーマットを行なうコマンド名は任意でよく、また必要な場合にはコマンド名に続きコマンドライン引数が後置される仕様でもよい。好ましくはこのコマンドの実体は別ファイルではなく、シェルの内部コマンドとして実装するのがよい。

【0047】ステップS13で、入力された文字列が記憶装置の初期化コマンドであった場合、ステップS14でサブCPU6内のリセットフラグ18の内容をクリアする。このクリア処理は、たとえばメインCPU9とサブCPU6を繋ぐ信号線を用いてメインCPU9からサブCPU6へ、開閉状態フラグ2をクリアするコマンドを発行することにより行なう。

【0048】ステップS15は、一般のシェルが備えている機能をそのまま実行する処理である。ここではファイルのコピーや外部コマンドの実行などを行なうが、もちろん、初期化コマンドがステップS12で入力された場合には、ステップS14で開閉状態フラグ2をクリアした後、指定された初期化処理を行なう。なお、ステップS15は単一のステップとして記載してあるが、ここでは、コマンド入力～実行のイベントループを実行してもよいし、また、単に1つのコマンド入力とその実行を行なうだけでもよい。

【0049】図5は、本携帯型電子機器のサブCPU6のアルゴリズムを示している。

【0050】サブCPU6には電源スイッチはなく、メ

イン電池11が装着されると直ちに動作を開始し、以後常に動作を続ける仕様になっている。そのため、図5に示したフローチャートでは処理の終了を意味するブロックがないが、これで問題はない。

【0051】また、メイン電池11から供給される電力はサブ2次電池8に充電されているため、メイン電池11を外していてもサブ2次電池8からの電力によって、サブCPU6は動作を続けることができる。

【0052】サブCPU6をステップS21から処理を実行させるには、前述の通りメイン電池11を装着する以外に、リセットスイッチ3を押下しリセットベクタから再起動することでも可能である。

【0053】ステップS22で、サブCPU6内のリセットフラグ18をセットし、リセット起動した旨を記憶する。この情報は、後にメインCPU9から情報取得コマンドが送られてきた際にメインCPU9へ通知される。

【0054】不図示の初期設定処理などを行った後、サブCPU6はステップS23でHALTモードへ移行する。このHALTモードはサブCPU6の消費電力を低くするモードとしてCPUチップに実施されている公知のものでよい。通常、HALTモードでは、動作に必要なクロック信号の停止、外部バスへのアクセス禁止などが行なわれる。HALTモードではサブCPU6は、電源スイッチ7からの押下信号を割り込み入力で待機している。

【0055】電源スイッチ7からの割り込み信号が通知されると、ステップS24でメイン電源管理装置10へ電源供給開始の指示を出し、メインCPU9の動作を開始させる。以降は、メインCPU9から信号線を経由して送られてくる各種コマンドに対して応答するという処理を実行する。リセットフラグ18の内容を取得するコマンドも、ここで入力、処理される。

【0056】ステップS25で、メインCPU9から入力されるコマンドを取り込み、ステップS26で、この内容を解析する。解析の結果、電源オフ要求コマンドではなかった場合は、その内容に応じた処理をステップS29で実行した後、再度ステップS25へ進み、コマンド入力待ちになる。メインCPU9から入力されたコマンドが電源オフ要求コマンドの場合はステップS27へ分岐する。

【0057】ステップS27は、前述のステップS24と同様に、メイン電源管理装置10へ電源供給終了の指示を出しメインCPU9の動作を終了させる。

【0058】ステップS28は、サブCPU6内のリセットフラグ18をクリアし、以降はリセット起動していない旨を記憶する。その後、サブCPU6の処理は再びステップS23の低消費電力モードに移行する。

【0059】次に、以上のような本実施形態の携帯型電子機器の運用について具体的に説明する。

【0060】まず、本携帯型電子機器が工場で組み立てられて一番初めに電源が投入された時は、図3のフローチャートにおいては、ステップS01→ステップS02→ステップS05→ステップS06→ステップS07→ステップS09→ステップS10となり、すぐに電源がオフされる。

【0061】そこで次に、リセットスイッチ3を押下してから電源を投入すると、ステップS01→ステップS02→ステップS03→ステップS06→ステップS07→ステップS08となり、シェルが起動する。ここで、初期化処理を行なうと、ステップS14で筐体開閉状態フラグ2がクリアされ、ステップS10で終了する。

【0062】次に電源をオンすると、ステップS01→ステップS02→ステップS03→ステップS04→ステップS10となり、以降は全く普通の操作が行え、ユーザにはこの状態で出荷される。

【0063】ユーザは、出荷された本携帯型電子機器に対して必要であればアプリケーションプログラムを追加し、さらに自己の運用に必要なデータ（パスワードや個人情報など機密性の高いものも含まれる）をRAM15にインストールし、業務に利用する。

【0064】ここで筐体を開けるとサブCPU6内の筐体開閉状態フラグ2がセットされ、次に電源を投入した時、ステップS01→ステップS02→ステップS03→ステップS06→ステップS07→ステップS09→ステップS10となりすぐに電源が切れてしまう。つまり悪意を持ったものが携帯型電子機器を分解して内部に細工を施しても、次からは2度と起動しなくなる。

【0065】ただし、この筐体を開けるという行為は正規のメンテナンス時にも必須の作業であり、このまま2度と使えなくなってしまうというのは非常に使い勝手が悪い。

【0066】しかし、本実施形態によれば、リセットスイッチ3を押下した後、電源を投入するとステップS01→ステップS02→ステップS03→ステップS06→ステップS07→ステップS08となり、シェルが起動する。この時点で、シェルからRAM15の内容を初期化するコマンドを実行すると、筐体開閉状態フラグ2がクリアされ、以降は再び通常起動および運用が可能になる。

【0067】以上のように、本実施形態によれば、機器の筐体を開放した場合は、機器の内部データを破壊し、筐体開閉状態フラグをセットすることにより、以後、通常の起動方法では2度と装置を起動できないように制御する。これにより、機器の記憶装置に格納されたパスワードや個人情報などを確実に保護できる。本実施形態によれば、内蔵されていたアプリケーションのリバースエンジニアリングや機密情報を盗み出すことは不可能となる。

【0068】また、機器の筐体を開放したとしても、リセット操作を行なった後、電源を投入すれば、シェルを起動することができ、ここで記憶装置の初期化操作を行なえば、記憶装置の初期化を実行するとともに筐体開閉状態フラグをリセットできるので、通常の起動操作を再び有効とし、容易に機器を再運用可能な状態に戻すことができる。

【0069】本実施形態においては、機器の筐体を開放した場合は、機器の内部データを無条件で破壊し、かつ、通常の起動操作を可能とするためには記憶装置の初期化を実行しなければならないので、たとえサービスマンが悪意をもって顧客のデータを盗もうとしてもそのような不正な内部データアクセスは一切行なえない。

【0070】なお、図4の制御において、ステップS13で初期化コマンドが指令されなかった場合はステップS15に移行するようにしているが、ステップS13で初期化コマンドが指令されなかった場合は処理を中止し、電源を遮断するようにしてもよい。つまり、初期化コマンドを実行した場合のみ、開閉状態フラグ2のクリアとコマンド実行（ないしコマンド実行ループ）を許容するようにする。あるいは、ステップS13で初期化コマンドが指令されなかった場合は、ステップS15に移行できるが、ステップS15で実行できるコマンドに制限を加えるようにしてもよい。

【0071】〔実施形態2〕先の実施形態では筐体が開けられた場合、ステップS06においてメモリ内データを全て00でクリアする、または、RAM電源管理装置17からRAM15へ供給されるバックアップ電源を切ることでRAM15の内容を破壊していた。これは、ステップS08でシェルを起動した際に、複写コマンド（たとえば、MS-DOSではCOPYコマンド）を使って、RAM15内のファイルをインターフェース12を介して外部記憶装置に複写されてしまうことを防ぐためである。

【0072】ところが、実際にはメモリ内データを全て00でクリアするには若干の時間が必要になる。特に近年の大容量のメモリを積んだ携帯型電子機器においてはかなりの時間を要する場合もある。また、RAM15への電源供給を管理するRAM電源管理装置17を設けることは電子機器の製造コストアップに繋がるため、好ましくない。

【0073】そこで、本発明第2の実施形態では上記問題を鑑みて、以下の処理を行なう。

【0074】まず、図3の中からステップS06（データ破壊処理）を除去したものが、第2の実施形態のメインCPU9のアルゴリズムとなる。本実施形態のメインCPU9のアルゴリズムは、それ以外では図3と全く同様であるものとする。

【0075】図6は本実施形態のシェルのアルゴリズムを示している。ステップS31からステップS36まで

は、それぞれ前述の図4のステップS11からステップS16と同じ機能であるため、説明は省略する。

【0076】図6では、ステップS33で入力されたコマンドが初期化コマンドではなかった場合はステップS37に分岐する。ここでは、更に入力されたコマンドが複写コマンド（たとえば、MS-DOSではCOPYコマンド）かどうかを調べ、複写コマンドではなかった場合ステップS38へ分岐する。しかし、複写コマンドの場合は何もせずステップS36へ分岐してそのまま終了する。

【0077】ステップS38では、入力されたコマンドが（シェルの内蔵コマンドではない）外部コマンドかどうか調べ、外部コマンドではなかった場合、ステップS35へ分岐し、そのままコマンドを実行する。しかし、外部コマンドの場合は何もせず、ステップS36へ分岐してそのまま終了する。

【0078】このようにして、図6で示すようにシェルを実装しておくことにより、図3のステップS06がなくても、電子機器の内部データを複写することができなくなるので、これにより電子機器の内部データを保護することができる。本実施形態では、データ破壊を行わないので、RAM電源管理装置17、あるいは少なくともそのデータ破壊機能は不要であり、製造コストを低減し、また、筐体開放時のタンパーブープ動作は筐体開放フラグのセットだけで済むのでより迅速に実行できる。

【0079】本実施形態2の構成によれば、電子機器の内部データを消去せず、その複写を行なえなくするようにしている他に、専用のプログラムを用意しても内部データをバックアップコピーすることはできない。

【0080】なお、筐体を開放した後は通常の起動が不可能となり、リセット操作によりシェルを起動し、そこで初期化コマンドを入力することにより再運用可能な状態に復帰させる動作については、上記実施形態1と同様である。

【0081】以上では、ディスプレイとキーボードを有する小型の携帯型電子機器を例示したが同様の技術は携帯電話機やPDA、ICカードなど内部に保護すべきデータ（パスワード、個人情報、あるいは企業秘密を含むアプリケーションプログラム、プログラムデータなど）を記憶する電子機器に広く実施することができる。また、以上ではシェルとしてsh、csh、command、comなど、コマンドラインインターフェースを用いるものを例示したが、シェルのユーザーインターフェース方式は任意であり、GUIを用いたものであってもよい。また、本発明に関しては、シェルは少なくともリセット後のメンテナンス作業で利用できればよく、通常の起動後、ユーザがこのシェルを用いて装置の操作を行なう構成でなくてもよいのはいうまでもない。

【0082】本発明の制御プログラムは、ROM14な

どに格納して装置とともに供給することができる他、ネットワークやインターフェース12を介してダウンロードすることによりインストールやアップグレードが行なえるような構成であってもよい。また、以上ではCPUがメイン/サブの2つに分かれた構成を例示したが、このような複数CPUの構成は必ずしも必須のものではない。

【0083】

【発明の効果】以上の説明から明らかなように、本発明によれば、筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムにおいて、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていないければ装置の通常起動を禁止する構成を採用しているもので、いったん筐体が開放されると、以後、装置の通常起動を禁止することにより、内部データの取り出し、リバースエンジニアリングなどの不正な装置の使用を防止できるとともに、リセット操作手段によりリセット操作を行なえば所定のユーザーインターフェースを介した装置の操作が可能となるため、装置のメンテナンスを行なうことができ、電子機器の耐タンパー性とメンテナンス性を両立できる、という優れた効果がある。

【0084】あるいはさらに、前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットする構成を採用することにより、内部のデータ記憶装置の初期化を条件として装置の通常起動を行なえるよう復帰させることができる。

【0085】あるいはさらに、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する構成、あるいは、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する構成によれば、確実にデータ記憶装置のデータ内容を保護することができる、という優れた効果がある。特に、内部のデータ記憶装置の内容を破壊せず、複写の禁止のみを行なう構成においては、ユーザデータを損なうことなく装置の修理/保守作業を行なえる、という利点がある。

【図面の簡単な説明】

【図1】本発明を採用した携帯型電子機器のブロック図である。

【図2】図1の携帯型電子機器の外観図である。

【図3】本発明の第1実施形態の電源投入時の制御を示したフローチャート図である。

【図4】本発明の第1実施形態のシェルの制御を示したフローチャート図である。

【図5】本発明の第1実施形態のサブCPUの制御を示したフローチャート図である。

【図6】本発明の第2実施形態のシェルの制御を示したフローチャート図である。

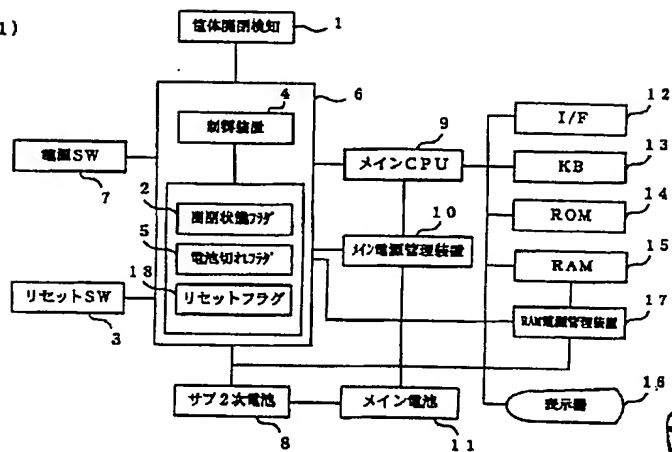
【符号の説明】

- 1 筐体開閉検知スイッチ
- 2 筐体開閉状態フラグ
- 3 リセットスイッチ
- 4 制御装置
- 5 電池切れフラグ
- 6 サブCPU
- 7 電源スイッチ

- 8 サブ2次電池
- 9 メインCPU
- 10 メイン電源管理装置
- 11 メイン電池
- 12 インターフェース
- 13 キーボード
- 14 ROM
- 15 RAM
- 16 表示器
- 17 RAM電源管理装置
- 18 リセットフラグ
- 20 下ケース
- 21 上ケース

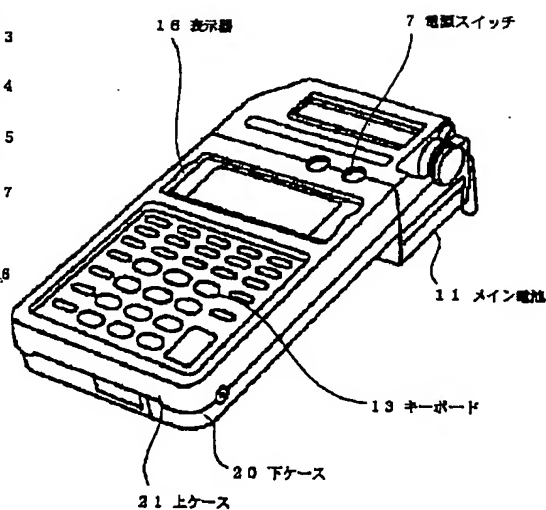
【図1】

(図1)

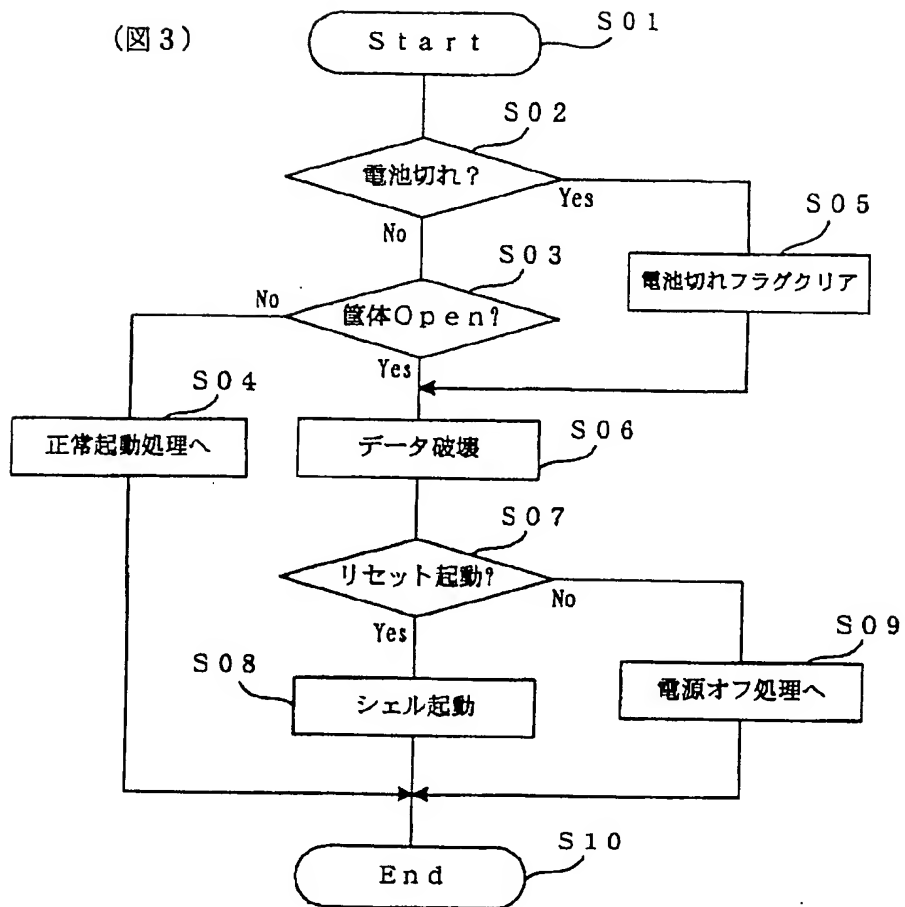


【図2】

(図2)

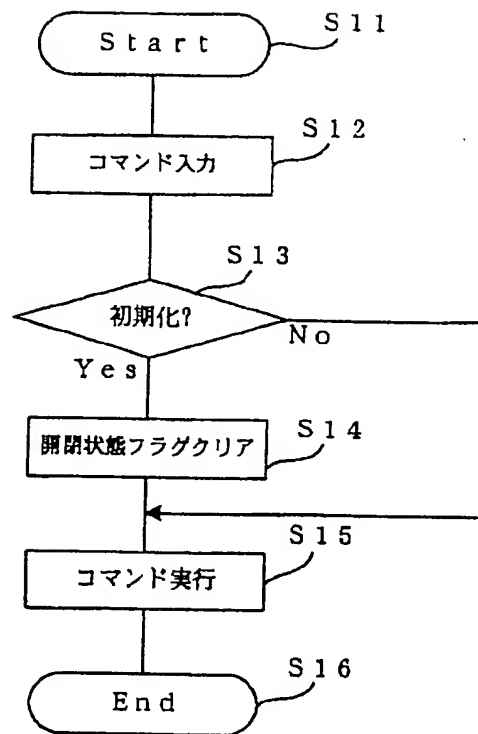


【図3】

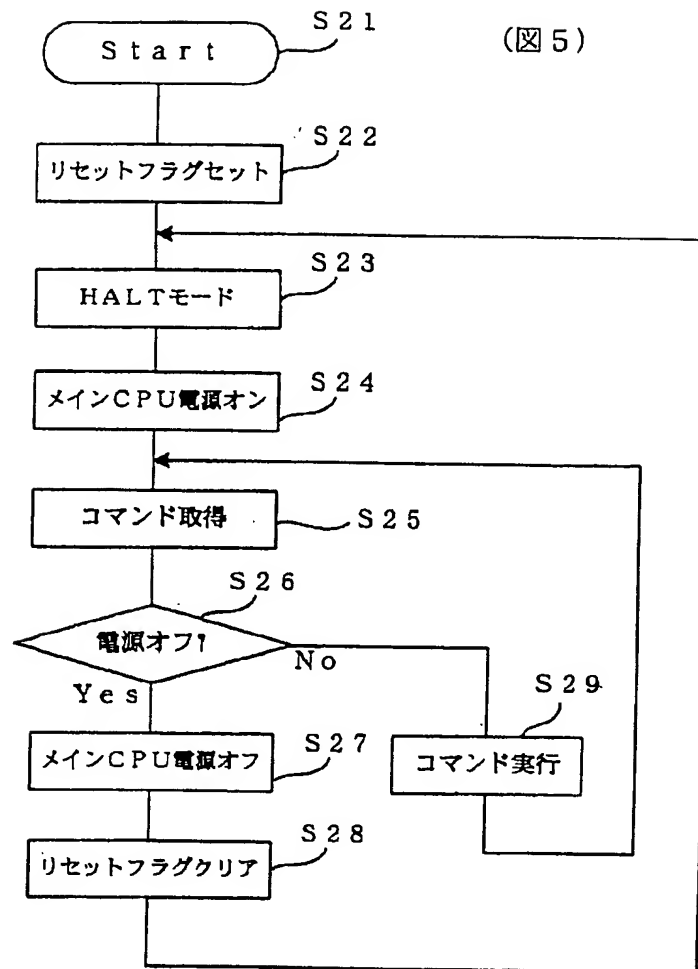


【図4】

(図4)



【図5】



【図6】

(図6)

